Integración de Redes Neuronales y Sistema de Detección de Intrusos (IDS), para las Amenazas y Ataques a los Sistemas de Información y Redes

Univ. Brenda María Alanoca Paco
dita_newage@hotmail.com

RESUMEN

Se quiere dar a conocer de forma clara y concreta la integración que existe entre Redes Neuronales y los Sistemas de Detección de Intrusos (IDS), su ayuda a los Sistemas de Información contra los ataques y amenazas. Además de realizar un análisis de las ventajas y desventajas que tiene dicha integración en los sistemas de información con respecto a su seguridad y las falencias que estas presentan al encontrarse con dichos intrusos.

PALABRAS CLAVES

Redes Neuronales, Sistemas de Detección de Intrusos (IDS), Sistemas de Información, ataques, amenazas, Red, Seguridad e intrusos.

1. INTRODUCCIÓN

Toda esta información debe de algún modo ser asegurada contra fugas, mientras que los equipos que hospedan o gestionan servicios deben ser protegidos contra accesos no autorizados o usos indebidos. Incluso cada computador asociado corre el riesgo de ser víctima de la visita inesperada de virus tipo gusano o intrusiones directas en su sistema operativo.

En un mundo donde la información es poder, es vital implementar sistemas de protección, detección y reacción de alta disponibilidad que puedan hacer frente a las amenazas del mundo exterior de la forma más efectiva posible, y con la intervención mínima de un administrador humano. Ante este desafío se puede encontrar una gran gama de soluciones en el mercado, que poseen diferentes características, pero que adolecen de una de las más deseadas: la adaptabilidad. Una buena parte de los productos funcionan basados en reglas actualizadas cada vez que aparece un nuevo ataque o variante de alguno ya existente. Algunos usan métodos estadísticos para determinar qué tanto se aleja el comportamiento de los usuarios en determinado momento de la conducta usual; la falencia común

sigue siendo la gran necesidad de administración ocasionada por las constantes actualizaciones y la generación de falsas alarmas debido a la poca adaptabilidad de los programas.

En este sentido se han planteado respuestas desde el punto de vista de la Inteligencia Artificial, que básicamente proponen que se puede identificar no sólo un ataque, sino todo un patrón de comportamiento asociado a él. Es el caso de las Redes Neuronales que no requieren ningún tipo convencional de tratamiento algorítmico para tal detección, aparte del necesario para filtrar la información del medio y convertirla en entradas

entendibles para la red (proceso también conocido como *codificación de entradas*).

Es así que nos hacemos la siguiente pregunta:

¿Existe una mejora sustancial al construir un sistema de detección de intrusos aplicando redes neuronales?

Los sistemas de detección de intrusos son herramientas que han sido diseñadas para aumentar la seguridad de una red de datos. Los estudios realizados en esta área tuvieron su origen en el análisis de los flujos de datos de los sistemas vulnerados, inicialmente personal experto en el tema dedicó todo su tiempo a identificar el origen de las anomalías y evitar que afectara de nuevo al sistema de información, esto evolucionó en lo que se conoce como sistemas de detección basados en reglas, que han sido estándar hasta la actualidad.

Los sistemas basados en reglas requieren actualización permanente ya que si un ataque es modificado levemente el sistema es incapaz de detectarlo. Por esto la inteligencia artificial se ha planteado como una solución a las limitaciones de los sistemas tradicionales.

A continuación se mostrarán los pasos que fueron necesarios para obtener un sistema de detección de intrusos basado en redes neuronales.

2. PREPARACIÓN DE LOS DATOS

Antes de comenzar el diseño es importante realizar la preparación consistente de los datos para que tengan el formato necesario para servir como **información de entrada de una red neuronal.** Para esto se ha realizado tres pasos que se describirán a continuación:

2.1 Conversión a formato decimal

En primer lugar las cadenas de caracteres, que actualmente se encuentran almacenadas en este formato, deben ser convertidas a un valor decimal, de tal forma que obtengamos una nueva cadena de valores ASCII correspondientes a cada una de las letras de la cadena de caracteres original. Por ejemplo, la siguiente cadena que representa un ataque de inyección de comandos '@.cgi?@=%0a@', queda representada de la siguiente forma:

[64 46 99 103 105 63 64 61 37 48 97 64]

De esta manera todas las cadenas de caracteres pueden ser manipuladas como datos decimales que tengan significado numérico [TOR03].

2.2 Ventana deslizante

Posteriormente, debemos darnos cuenta que las cadenas decimales con las que contamos, suelen tener un tamaño variable, es decir que algunas tienen 5 elementos, otras12 elementos y en general la gran mayoría tiene un número variable de elementos. Si se pretende que estas cadenas sean entradas de entrenamiento para nuestra red neuronal, debemos considerar el hecho de que nuestra red neuronal posee un número de entradas fija, una vez que ha sido definido. De manera que si tiene un número fijo de 8 entradas no podrá procesar una cadena de 12 elementos. Para solucionar este problema, se diseñado una ventana deslizante, cuya labor es la de convertir las cadenas de tamaño variable, en cadenas de tamaño fijo, de manera que nosotros fijemos el número estático al que se deberá ajustar la longitud de todas las cadenas con las que contemos. Para esto imaginemos que poseemos las siguientes cadenas decimales:

120 33 45 64 32
23 34 45 67
88 90 14 57 10 13 45
24 15 12

Sabiendo que la cadena más chica tiene un tamaño de tres, se puede tomar este número como el tamaño fijo que deberán tener todas las cadenas. Así pues las cadenas anteriores quedarían representadas de la siguiente manera:

120 33 45
33 45 64
45 64 32
23 34 45
34 45 67
88 90 14
90 14 57
14 57 10
57 10 13
10 13 45
24 15 12

De esta manera se han generado cadenas de tamaño fijo al costo de generar más cadenas de entrenamiento, costo que en realidad es un beneficio extra al permitir a la red observar más patrones de entrenamiento con que poder generalizar.

2.3 Conversión a formato binario

Finalmente las cadenas decimales de tamaño fijo, deben ser convertidas a un formato que pueda generar los cambios suficientes para que en el rango de entrada de una neurona sigmoidea se genere el mayor cambio posible. Recordaremos que el rango de entrada de una neurona acepta cualquier valor de los números reales, sin embargo los cambios más significativos a la salida de estas neuronas, suceden cuando el rango de entrada está entre cero y uno. Esta es la principal razón para elegir que los números decimales con los que ahora contamos, que van desde 0 hasta 255, sean convertidos a formato binario para que se ajusten al rango de 0 y 1 necesario para que las neuronas trabajen adecuadamente y nos permitan que la variación en los pesos de la red neuronal, debido al entrenamiento, no sean tan drásticos. Así pues, las cadenas decimales de tamaño fijo con las que contábamos como pudieran ser las siguientes:

64 37 42
37 42 33
43 28 96
28 96 41

Serán transformadas a formato binario quedando de la siguiente manera:

01000000 00100101 00101010
00100101 00101010 00100001
00101011 00011100 01100000
00011100 01100000 00101001

Ahora solo basta definir el modelo de red neuronal más adecuado para solucionar el problema en cuestión referente a la detección de Intrusos en redes de comunicación y los sistemas de información.

3. DISEÑO Y ENTRENAMIENTO DE LA RED NEURONAL

Una vez que se ha definido el número de entradas de la red neuronal igual a 64 se puede definir también el número de salidas necesarias para representar las cinco clasificaciones posibles que nuestra red neuronal debe tener. De esta manera determinamos que el número de neuronas de salida sea igual a cinco, tomando en cuenta que cada neurona sea destinada a activarse cuando el dato en la entrada de la red neuronal corresponda a un tipo de clasificación, y que las demás neuronas se encuentren desactivadas cuando el dato a la entrada no pertenezca a la clasificación determinada por la neurona. En otras palabras, cada una de las cinco neuronas debe corresponder a una de las cinco posibles clasificaciones de manera que cuando el dato a la entrada pertenezca a una de estas clasificaciones, la neurona correspondiente a esta clasificación sea activada y las demás sean deshabilitadas.

Para esto, se ha diseñado en el código IDS2, del código fuente, que la primera neurona de salida se active cuando el dato a la entrada sea de tipo NORMAL, la segunda neurona deberá activarse cuando el dato a la entrada sea de tipo ATAQUE POR INYECCION, la tercera neurona deberá activarse cuando el dato a la entrada sea de tipo ATAQUE POR MODIFICACION DE PATH, la cuarta neurona debe ser activada cuando el dato a la entrada sea de tipo ATAQUE POR INYECCION SQL, y la quinta neurona debe ser activada para cuando el dato a la entrada corresponda a un ATAQUE POR XSS (Cross Site Script). Recordando que cuando una neurona este activada o en valor alto o en uno, las demás deberán estar en valor bajo, o cero.

Así un sistema basado en redes neuronales permite detectar nuevos paquetes peligrosos a partir del conocimiento previamente adquirido, lo que no sucede con los sistemas no basados en redes neuronales. Esto permite que el administrador de una red se

convierta en un contribuyente de conocimiento y no simplemente en un usuario de sistemas de detección de intrusos.

La aplicación de redes neuronales para la detección de intrusos en redes informáticas puede ser de gran apoyo para los sistemas de detección tradicionales gracias a su capacidad de generalización y aprendizaje.

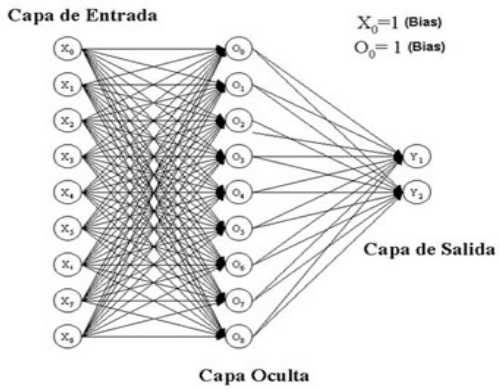

Fig.1

4. VENTAJAS Y DESVENTAJAS

Ventajas de usar RNA en IDS

• La red aprenderá de manera autónoma a partir de los ejemplos, lo que disminuirá el tiempo y esfuerzo del proceso de "finetunning" que se necesita para su correcto funcionamiento
• La red neuronal artificial se puede adaptar a nuevos comportamientos, la cual hace al sistema mucho más flexible a variaciones y modificaciones de los métodos de intrusión actualmente conocidos (Base de conocimiento)
• Disminuir la cantidad de falsos positivos y falsos negativos que presentan los sistemas IDS basados en firmas
• La red infiere ataques que no aprendió, y puede adaptarse a los que el administrador de red cual lo convierte en un sistema, de cierta manera, heurístico.
• El éxito de un sistema de redes neuronales se basa en el entrenamiento y en la selección de un universo adecuado y familiar a la red donde se planea utilizar el sistema.

Desventajas

• Variabilidad del sistema
• Posee muchos parámetros configurables y esto crea muchos problemas a la hora de hacerle finetunning.
• La representación de los datos para que el sistema opere con ellos, y su adquisición por medio de los elementos de E-box • Posible pérdida de información discriminante valiosa al hacer conversión de datos
• Poca o nula trazabilidad de los ataques.

5. CONCLUSIONES

• El desarrollo de IDS es un complejo campo que debe ser abordado con una perspectiva que ayude a enfrentar el problema gigante que representa la seguridad de la información, es por esta razón que se hace necesario abordar el problema de manera distinta a la que se usa actualmente, una opción para hacerlo son los sistemas inteligentes, en nuestro caso las redes neuronales artificiales.
• Esta investigación y propuesta de modelo SIDIRI será desarrollada como trabajo de grado por los ponentes del presente artículo.

6. BIBLIOGRAFÍA

[1] PINACHO, Pedro Pablo; VALENZUELA Tito. Universidad de Santiago (Chile). Una Propuesta de IDS Basado en Redes Neuronales Recurrentes [en línea]. México DF, Octubre de 2003. [ref. de 13 de Marzo de 2007] http://www.criptored.upm.es/guiateoria/gt_m291b.htm

[2] "REDES NEURONALES ARTIFICIALES", José R. Hilera y Víctor J Martínez. 2000. Alfa omega. Madrid. España

[3] ``Intrusion Detection Systems". R. Bace, P. Mell. NIST (National Institute of Standards and Technology) http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf